外部認証機構と連携した動的なアクセス制御システムに関する一考察

佐藤 大輔* 中原 慎一*
* 日本電信電話株式会社 情報流通基盤総合研究所

1.はじめに

現在、Web 向けシングルサインオン(SSO)製品に代表されるように、保護対象リソースへのアクセス制御とユーザ認証を連携させたシステムがイントラネットのみならずエクストラネットにも導入されてきている[1]。現在は Web サービスがメインであるが、今後ブロードバンドサービスの拡大が予想される中で、例えばエクストラネット上で VOD サービスやライブ配信といった動画配信サービスや各種コミュニケーションサービスなど多種多様なサービスを一纏めに提供するポータルサービスなどへの SSO の適用を考えた場合、現行の主な方式を適用しただけでは、多様なサービスを吸収できる幅広い動作環境をカバーすることと、大容量データの流通に伴う負荷を分散させることを両立させることができない。本稿では、現行方式の比較検討を行うことで上記問題点を示し、その解決案として、ルールベースの動的変更が可能なファイアウォール(以下 FW)と外部認証機構を連携させる新たな NW 上リソースへの動的アクセス制御方式を提案し、考察を行う。ルールベースとは、FW 上でのセキュリティポリシの実現手段である。

SSO の概念を実現するシステムは多数存在する[1]が、本論文で述べる SSO のシステムは、複数のアプリケーションサーバへのアクセス制御を一元的に行う仕組みを持ち、管理者が設定したアクセス制御リスト(ACL)に基づいて、ユーザ毎に各リソース(サーバ)に対して「ユーザ認証」と「アクセス制御」を行うシステムであるとする。ここでは、「ユーザ認証」とは登録された利用者本人であることを確認する手段を意味する。また「アクセス制御」は登録利用者内での権限のチェックを行う「アクセス権限チェック」と、アクセス権を持たない第 3 者からの不当なアクセスの防止を目的とした「通過制御」の 2 つの機能からなるものとする。特に「通過制御」には、FW で実現される不特定多数を対象としたもの(以下、こちらを単に通過制御と呼ぶ)と、「アクセス権限チェック」によるチェックをクリアしたユーザのみについて通過を許可する「SSO 内通過制御」の 2 つが存在する。

2.ユーザ認証とリソースへのアクセス制御方式

2.1.現行方式の比較

現行の SSO システムの実現方式は主に 2 タイプに分けることができる。1 つは、プロキシサーバの仕組みを利用したリバース・プロキシ方式であり、もう 1 つはアクセスの対象とする Web サーバ(リソース)に専用のエージェントモジュールを組込むエージェントモジュール方式である。両方式の特徴を図 1-A,B に示す。

2.1.1 リバース・プロキシ方式

図 1-A に示すようにリバース・プロキシ方式では、登録された利用者本人であるかどうかを判定する「ユーザ認証」と、ユーザのリソースに対する「アクセス権限チェック」と、そのアクセス権限の有無を判断して行う「SSO 内通過制御」とを、すべて SSO サーバが担当する構成をとる。以上の処理が FW による「通過制御」の後に行われる。この方式では SSO サーバがプロキシサーバとして一元的にアクセス制御を行うため、サービス内容や保護リソースの機種に依存しない制御ができる反面、保護対象サーバへのすべてのアクセスが集中し、かつすべての機能が直列に構成されていることから負荷の集中が問題となる。特にシステム構成において SSO サーバを一台しか配置しない場合は別ドメインの保護対象サーバに関するアクセスも集中する。ブロードバンドサービスの拡大が予想される中で、映像データなど大容量のデータが集中することは重大な問題となる。また、各ドメインに 1 台 SSO サーバ、またはその機能を代行するバーチャルサーバを導入する構成をとる場合もあるが、この場合は各 SSO サーバ間の同期、連携が必要であり、構成が複雑化するという欠点を持ち、各ドメインの FW と直列に配置されるため「通過制御」に関する通信ネックが全ドメインで 2 重に発生することになる。

2.1.2 エージェントモジュール方式

図 1-B にエージェントモジュール方式の構成を示す。この方式では、SSO サーバが「ユーザ認証」と「アクセス権限チェック」を行い、クッキー及びリソースサーバに配置する専用のアクセス制御モジュールを用いて「SSO 内通過制御」を行う。この方法では、「ユーザ認証」「アクセス権限チェック」と「SSO 内通過制御」、FW による「通過制御」が並列となり、リソースへのアクセス時に SSO サーバを経由する必要はないためリバース・プロキシ方式に比べアクセス負荷を分散し軽減する効果がある。しかし、各保護対象サーバすべてに専用のエージェントモジュールを組み込む必要があるため、リバース・プロキシ方式に比べ構築と管理の負担が大きいことと、アクセス制御時にクッキーを利用するため、HTTP プロトコルを利用するサービスにしか対応できず、多様な動作環境をカバーすることができない、という欠点を持つ。

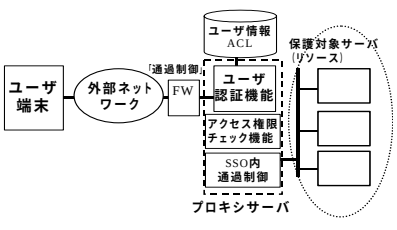

図 1-A リバース・プロキシ方式 SSO

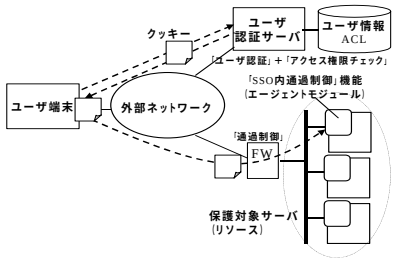

図 1-B エージェントモジュール方式 SSO

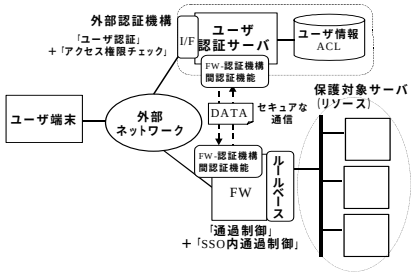

図 1-C FW-認証機構連携方式 SSO

表 1 SSO 各方式比較

SSO実現方式		リバース・プロキシ方式	エージェントモジュール方式	FW・認証機構連携方式
保護対象サーバ条件	プロトコル	問わない ○ サービス毎に設定が必要	制限あり × クッキー使用のためHTTPのみ	問わない ○
	サーバ種別	問わない ○	制限あり × エージェントモジュール インストールのため	問わない ○
アクセス負荷		SSOサーバに集中する × 全ての接続がSSOサーバ 経由で行われるため	各ノードに分散する ○	各FW単位で分散する △
システム構成の容易さ		SSOサーバ1台なら容易○ 複数台設置の場合複雑×	保護対象サーバすべてモジュール インストールが必要 ×	認証機構の構築のみのため、 容易 ○

以上のように、現行の方式では

①アクセス負荷の集中によるボトルネック

②保護対象リソースの提供形態や、サーバソフトなどの動作環境に関する制限

の 2 点が主な問題であり、上記 2 方式では両問題の解決がトレードオフの関係にあるため、双方を解決する新たな方式が望まれる。

2.2. ファイアウォール-認証機構連携方式

本研究では、「ユーザ認証」と「アクセス権限チェック」を外部認証機構で行い、FW のルールベースをリモートかつ自動での編集を可能にし、外部認証機構と FW との間にセキュアな通信機能を設けることでセキュリティポリシの動的で安全な変更を可能とする方式を提案する。これによって前述した問題について、以下のように解決できる。

①アクセス負荷の集中によるボトルネック

FW のセキュリティポリシを動的に変更可能にすることにより「通過制御」だけでなく「SSO 内通過制御」もまとめて FW で行うことが可能となり、機能の並列配置による負荷分散が図れる。

②保護対象リソースの提供形態、動作環境に関する制限

エージェントモジュール方式では HTTP プロトコルにしか対応しないエージェントモジュールによって実現していた「SSO 内通過制御」を、プロトコルやアドレス、ポート番号など多数の情報に対応できるセキュリティポリシが設定可能な FW を利用して動的に行うことで、幅広い動作環境をカバーすることが可能となる。

本方式の構成を図 1-C に、現行の 2 方式と本方式の比較を表 1 に示す。

3.機能の検討

FW-認証機構連携方式を実現するには、認証機構と FW に図 2 に示すような機能が必要と考えられる。本システムにおいて特に重要なのは、FW と認証機構の間でセキュアにデータのやりとりをするための FW-認証機構間通信での漏えい防止機能と、認証機構でユーザ認証に成功したユーザに関して FW を通過させるようにルールベースを変更し、接続終了後にルールベースを元に戻すことでユーザに対するアクセス制御を行うルールベース編集関連の機能であり、以下各機能について述べる。

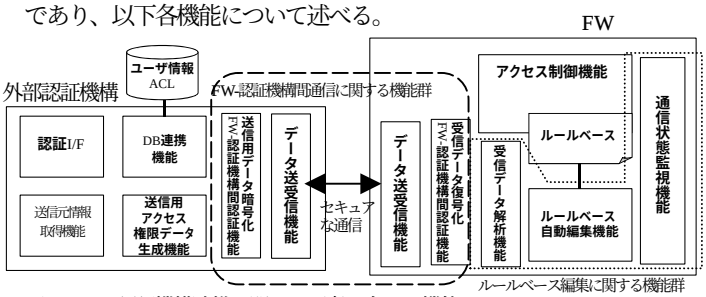

図 2　FW-認証機構連携に関する両者の有する機能

3.1.FW-認証機構間通信に関する機能

本システムでは、外部から FW のルールベースを設定可能にするため、外部認証機構と FW との間の通信は極めてセキュアに行わねばならない。そこで、通信を暗号化する以外にも、ユーザ認証とは別にFW-認証機構間についても相互間で専用の認証を行うことを特徴とする。

暗号化、認証の方式としては、現在市販されている FW の多くが対応している IPsec による VPN を用いれば、認証機構側では FW 側に対して特に新しくアプリケーションのインストールなどを要求することなく実現が可能である[2]。その上で、サイトの目的やセキュリティポリシに合わせ、公開鍵暗号方式によるデジタル署名やワンタイムパスワードなどを追加することにより、なりすましから情報漏洩、改ざんなどに対してよりセキュリティ強度を上げていくことができる。

3.2. ルールベースの編集に関する機能

3.2.1 ルールベース自動編集機能と通信状態監視機能

ユーザ認証に成功したユーザが目的のリソースを提供するサービスにアクセスしてきた際に、このユーザからのアクセスを指定してきたサービスに関して許可するようにルールベースを自動的に編集する機能を FW に付与する。また、ルールベースをある特定のユーザからのアクセスを許可する状態のまま放置すると、そのユーザを詐称する「なりすまし」による攻撃を受ける危険がある。そのため、不要なルールはルールベースから逐次削除する必要がある[3]。理想的にはユーザが該当サービスを受けている間のみ接続を許可し、サービスの終了とともに該当ユーザの接続許可ルールを削除することが望ましい。そのため、FW にはユーザとリソースの間の通信状態を監視する機能を設ける。

本システムではユーザを特定する情報として送信元 IP アドレスを仮定する。認証機構において初期ログイン時にユーザの送信元ホストの IP アドレスを取得し、ユーザ認証成功時にユーザのアクセス権限データとともに FW へと送信する。受信した FW 側では、この IP アドレスからの指定サービスへのアクセスを許可するようにルールベースを変更する。

3.2.2 サービス終了検知方法

次に、サービス終了までのサービス状態の検知について述べる。

サービスの開始は、ユーザからの最初のパケットが通過を許可された際に検知される。ユーザがサービスへの接続を開始すると、まずタイマーがセットされタイマー処理がスタートする。

サービス継続を認識する方法として、接続中は FW はすべての着信および発信パケットを捕捉し、パケット内部情報を取得、解析、保存を行い、保存したパケット内部情報を時系列に従って累積させていくことで、通信状況を示す通信状態情報を構築する。この通信状態情報を新たに取得したパケット内部情報と照合することで通信の整合性を判断し、サービスが継続していると認識する。サービス継続と判断された時点で、タイマーは一度リセットされる。また捕捉したパケットを適宜サンプリングし、ルールに一致しているか検査する処理を組み込むことも考えられる。

サービス終了については、通信の終了を示すパケットを検知した場合に認識し、通信状態監視機能はルールベース編集機能へ該当ユーザの送信元 IP に対するアクセス許可ルール削除要求を出しルールベースを変更する。通信が異常終了した場合、基本的にはタイムアウト処理を行い、タイムアウトを以ってサービス終了と認識する。

本例では、アクセスユーザに対するルールベース変更を示したが、同様にプロトコルやアプリケーションなどをキーに動的な通過制御が外部から可能となる。

4.まとめと今後について

本論文では、ブロードバンドサービスをはじめとする多様なサービスを対象とした SSO システムについて、現行 SSO 方式を比較することで問題点を挙げ、その解決案としてルールベースを外部から動的に変更可能な機能を有する FW とユーザ認証機構を NW を通して連携させることで SSO を実現する方式を提案し、その優位性と実現可能性について考察した。

今後は、FW－認証機構間の認証方法についてより詳細な検討を行い、各機能を実装し、評価を行う。

【参考文献】

[1]日経インターネットテクノロジー,2001.4,p190-199.

[2]Checkpoint 製品 導入の手引き,2000.

[3]小林他,ダイナミックフィルタリングを利用したパーソナルファイアウォールの設計, 情処学会研究報告,2002,No.12,pp151-156.

[4]中村他,IDS と Firewall を連携した Dynamic Firewall の実装と評価 ,信学技報,Vol.101,No.649,pp35-40.

“A study on the dynamic access control of SSO system using FW and external authentication mechanism”

Daisuke SATO, Shinichi NAKAHARA

NTT Information Sharing Laboratory Group ,Nippon Telegraph and Telephone Corporation